(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 January 2002 (31.01.2002)

PCT

(10) International Publication Number
WO 02/08865 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US01/23264

(22) International Filing Date: 24 July 2001 (24.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/220,265 24 July 2000 (24.07.2000) US

(71) Applicant and
(72) Inventor: CHAUM, David [US/US]; 14652 Sutton St., Sherman Oaks, CA 91403 (US).

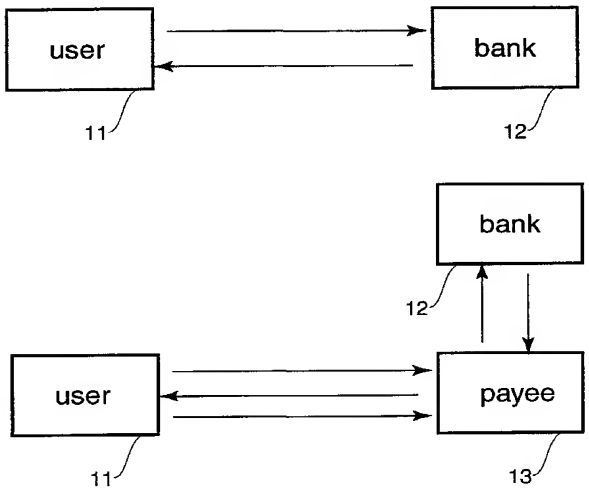
(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: TRANSPARENT-COIN ELECTRONIC MONEY SYSTEM



(57) Abstract: Digital transaction systems are disclosed that allow, in some exemplary embodiments, the transfer of value from at least one party to at least another party through one of plural intermediate parties. During the transactions between an intermediary and another party to the system, the intermediary can change the way the value held is denominated without revealing whether such a transformation has actually taken place. In some examples, the intermediary may split an "electronic coin" of one value into two, each having half that value. The intermediary would be able to choose, however, whether or not the value was in fact split or the transaction was a dummy and this choice would be hidden from the other parties. Similarly, an intermediary can optionally combine two tokens of value into a single token of twice the value, without revealing whether or not the transformation was actually conducted with items of value or simply with random numbers. In some electronic money systems it is desired that each payer can only transform value into forms that they can trace. Such restrictions are provided for in embodiments that ensure that any new item of value is derived from pre-committed items.

WO 02/08865 A2

TRANSPARENT-COIN ELECTRONIC MONEY SYSTEM

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates generally to digital transactions, and more specifically to secure and/or privacy protecting techniques for exchange of value.

2. Description of Prior Art

The present application claims priority based on the United States Provisional Application titled "Hidden-Change Electronic Money," U.S. PTO 60/220265, filed 07/24/00 by the present applicant. Other related patents and patent publications by the present applicant, including "Blind signature systems," UP Patent 4,759,063, 7/19/88, "Returned-value blind signature systems," US Patent 4,949,380, 14/8/90, and "Optimistic authenticator systems," PCT Publication number WO 00/64088, 10/26/00, are hereby including by reference.

Known practical electronic cash systems have required payers to hold extra and unusable value in cash, which has been an impediment to widespread acceptance of the technology. Actually deployed electronic cash systems have required "exact change," thereby requiring unusable value to be held by the payer. Although they can be configured to ensure a configured minimum number of payments can be made for a given amount of cash held, generally considerable cash held by users remains inaccessible without conducting a change transaction. Moreover, this approach makes the underlying coin-based nature of the implementation hard to hide from users, a further factor working against adoption.

A less-obvious but nevertheless potentially significant aspect of many of these systems, which have been marketed as privacy protecting, is that they can reveal a surprising amount of information linking payers to payments. This is because all change transactions are conducted while the user is identified to the bank or, in some systems by temporal proximity, to a merchant. Although the exact linking between payments and users will not in general be revealed, some unique linkings, impossibilities of certain other linkings, and potentially revealing probabilities of yet other linkings may be inferable from the full history of payment and change requests.

Some elaborate cryptographic techniques have been proposed to address parts of these problems, but they have resisted actual practical use, introduced some of their own issues, and required very specific features of the underlying cryptographic primitives. One example of these techniques is the so-called "Returned-value blind signature systems" referred to above. The amount of money that must be kept in cash is actually increased under the more practical versions of that approach, by tying up an amount that is on average at least twice that of each payment to be made. A second example is the hierarchical schemes of Okamoto and Ohta, such as those described in US Patent 5,224,162, titled "Electronic cash system" and issued 6/29/93. Although they improve the ability to spend all cash held, this is achieved only by using impressive and so far impractical cryptography as well providing various new sources of linking information, not all of which are believed readily addressed. Additionally, various so-called "tick" payment systems have

been proposed (and re-proposed) for limited applications typically including only small amount payments, though they do not claim to practically address the general case of arbitrary amounts of payment.

A fundamental problem introduced by many of the above mentioned systems is their facilitation of, and inability to limit, so-called "payee anonymity". This has been argued elsewhere to allow criminal use of payments without payer accountability. The ability to restrict payee anonymity can be expected to be a legislated requirement for such systems that come into widespread use.

The present invention aims to overcome these problems and limitations of the prior art and has among its objects the following:

- Providing complete fungibility, thereby neither requiring payers to hold extra value nor preventing them from making payments for which they hold sufficient value;
- Hiding substantially each payer's pattern of denomination usage;
- Making only modest requirements of the underlying cryptographic primitives; and
- Allowing blocking of payee anonymity.

Yet other objects include practical, efficient, and convenient systems in accordance with the teachings of the present invention. Still other objects, features, and advantages of the present inventive concepts will be more fully appreciated when the following specification and appended claims are read with reference to the drawing figures.

BRIEF DESCRIPTION OF THE DRAWING FIGURES

Fig. 1a shows a combined block, functional, and flow diagram of interactions between a pair of parties for an exemplary embodiment in accordance with the teachings of the present invention.

Fig. 1b shows a combined block, functional, and flow diagram of interactions between a triple of parties for an exemplary embodiment in accordance with the teachings of the present invention.

Fig. 2 shows a combined block, functional, flow, and cryptographic-protocol diagram of interactions between a payer and a bank for an exemplary embodiment of a "maybemerge" transaction in accordance with the teachings of the present invention.

Fig. 3 shows a combined block, functional, flow, and cryptographic-protocol diagram of interactions between a payer and a bank for an exemplary embodiment of a "maybesplit" transaction in accordance with the teachings of the present invention.

Fig. 4 shows a combined block, functional, flow, and cryptographic-protocol diagram of interactions between a payer and a bank for an exemplary embodiment of a general merge and/or split transaction in accordance with the teachings of the present invention.

Fig. 5 shows a combined block, functional, flow, and cryptographic-protocol diagram of interactions between a payer and a bank for an exemplary embodiment of a preparatory transaction in accordance with the teachings of the present invention.

Fig. 6 shows a combined block, functional, flow, and cryptographic-protocol diagram of interactions between a payer and a bank for an exemplary embodiment in a "maybesplit" transaction, related to a preparatory transaction, in accordance with the teachings of the present invention.

BRIEF SUMMARY OF THE INVENTION

This section introduces some basic concepts of the invention, but makes significant simplifications and omissions for clarity, as will be appreciated, and should not be taken to limit its scope in any way; the next section presents a more general view.

In broad summary and a simplified example, two underlying innovative example transactions are the "maybemerge" and "maybesplit." The Maybemerge interaction either has no effect or it cancels the validity of two coins of the same denomination and validates a new coin with double that denomination. Only the payer can know whether it changes nothing or is actually a merge yielding a new coin in exchange for two. In either case, the total value remains the same. Similarly, a maybesplit is either a "no-op" or changes a single coin of one value into two, each of half the value of the split coin—without the bank learning whether it resulted in a split or was merely a dummy. More generally, a transaction can accomplish one of plural potential transformations between sets of coins having equivalent aggregate value without the bank learning which transformation(s) occurred. Moreover, the bank can prevent so-called "payee anonymity" by ensuring that all coins involved in an actual transformation are related to the same payer.

An exemplary illustrative way to realize a maybemerge, in overview, is as follows: The user provides two unauthenticated digital coins to the bank along with a blinded coin. If the maybemerge is to have no effect, then the payer can simply create all these values at random; in the other case, however, where an actual merge is wanted, the values provided are genuine and the user knows the authenticated form of the two coins revealed and is prepared to remove the blinding on the third number. What the bank does is first make sure that the coins have not been, and cannot later be, spent. When this is successfully done, the bank signs or otherwise authenticates the blinded number, but "combines" it with the authenticator values for the two coins. This combining preferably resists various attacks, such as the user being able to learn authenticators for any coin, except when the authenticators are known for both merged coins, and then only for the one new coin. For instance, an exemplary combining technique would apply independent one-way functions to the authenticators to be merged before multiplying them (in a homomorphic signature scheme) with the authenticator value to result from the merger.

An exemplary maybesplit can work similarly, although it can typically be expected to be conducted while, for instance, cryptographically tunneling through a payee to a bank. An unauthenticated coin and two blinded coins are supplied to the bank. Much as with a maybemerge, the bank cancels the coin to be split and returns appropriate signatures on the two blinded coins, each combined preferably independently with the authenticator of the unauthenticated coin values supplied.

One example way to use these primitives allows the user to conveniently maintain the coins held in a single "canonical" form and conduct withdrawal and payment transactions each in a uniform way. In a binary denomination scheme, where each denomination is worth twice that of the next lower denomination, at most one coin of each denomination is held in the canonical form. During a withdrawal, if the amount to be withdrawn yields a coin of a denomination already held, then the two coins can be merged. A sequence of merges from the smallest to largest denomination suffices to integrate a withdrawal amount that is itself in canonical form. In a related manner, during a payment, if certain denominations are needed, they can be formed by splitting the next larger denomination that is held. Again a series of splits over the whole range is believed sufficient for any achievable amount of payment.

In a system that aims to prevent payers from using coins that they have not previously committed to, it can make a difference whether the user is identified to the bank in the particular transaction. When the user is known to the bank, then the bank can require that any blinded coins used have been committed to previously because the have been previously supplied, such as by looking them up or requiring the user to supply an authenticated receipt. But when the user is preferably not identified to the bank, such as is preferable when the transaction tunnels through a payee, such a technique is not applicable.

An inventive solution detailed later allows the user to obtain "transformation values" from the bank when identified to the bank and to later use them when tunneled through a payee. These transformation values are formed in a way that allows recovery of partially-authenticated coins when certain special authenticators are known for a related coin. In a particular example, for a maybesplit, there are three blinded coins known to the bank, the double that is to be split into the two singles. During an earlier interaction, the bank supplies for each of the two singles an authenticator that can be opened only when a special authenticator is known for the double. During a payment, the bank supplies the special authenticator on the unblinded double cancelled as well as partial authenticators on the blinded singles. These partials can only be opened using the authenticator for the double and they provide the missing complementary part giving the singles the combined authenticators of the appropriate value.

GENERAL DESCRIPTION

The example systems already summarized will first be expanded on here generally to introduce some inventive concepts but without implying any limitation. The techniques can readily be applied to a variety of settings, not limited to financial transactions. Examples include, but without implying any limitation, games of chance and/or skill as well as loyalty schemes. For clarity of exposition and ease of understanding, as will be appreciated, but without implying any limitation, the terminology of financial transactions will often be used in the present specification, figures, and claims. Thus, for example, the terms user, payer, payee, bank, can be understood to be names for parties or their computational agents involved in transactions of whatever type; terms such as value, amount, denomination and so forth can be interpreted as relating to whatever quantities, not necessarily financial. The terms issuer of value, transacting party, and receiver of value, are used to denote the full generality of the potential parties herein described. The term setup relates generally to any data or derivative/precursor or related data that is pre-existing at a time after it has been established. Moreover, the term coin will be used to refer to any digitally encoded bearer form of value, no matter how encoded, what type of value, or what is required to issuer or redeem it.

Transactions can, for instance, be between the user and bank directly or between them through the payee. Many other arrangements are possible and would be in keeping with the present invention. For instance, but without limitation, the user could communicate with the bank substantially at the time of payment without going through the payee. If the transaction is related to a particular payment, temporal proximity of the transactions can, however, suggest a linking that can undermine privacy of the transaction. If an untraceable channel, such as might generally be provided or be provided through other parties is used, these issues can be addressed without tunneling through the payer.

One example way already mentioned to use such techniques, in an electronic money system with a binary denomination scheme, does not require the user to hold more than one coin of each denomination. Thus, when the amount of value held by the user is thought of as represented as a binary integer, each 1 bit corresponds to a coin held and each 0

bit to no coin for that denomination. Withdrawals can be for any amount, while payments can be for any amount less than or equal to the value held. During withdrawal, carry propagation may be required from any set bit in the amount withdrawn to the maximum digit required by the total amount held by the payer. For each such potential carry, a maybemerge sub-protocol is performed. Thus if the carry is needed, the maybemerge has the effect of creating a carry coin of the higher denomination. For payment, borrows are potentially required. And for each potential borrow, from the maximum set bit in the amount held, down to the two's bit, a maybesplit is used.

Transaction flows for each user can in one example be comprised of a series of interactions of two types: withdrawal of value from the bank and payment to merchants. In between these transactions, the user holds at most one coin of each denomination. During a withdrawal, a set of coins is withdrawn in a canonical form that represents the exact amount withdrawn, which can be any amount. A set of merge operations is done, one for each potentially effected digit (preferably up to some agreed total maximum to be held), resulting in the user's coins being in a canonical form. During a withdrawal, a series of split operations is done, one for each digit potentially involved (preferably up to some agreed total maximum held), resulting in the set of coins needed for the payment and the remaining coins in canonical form.

Binary denomination schemes are used in the examples for clarity. A wide variety of denomination schemes can, however, be used with the present inventive concepts. A tertiary scheme, for instance without limitation, would work in a similar way as would be appreciated, except that instead of pairs of coins, triples would be used. Less homogenous schemes can of course also be used, as would be appreciated by those of ordinary skill in the art.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Turning now to Fig. 1, combined block, functional, and flow diagrams are presented for exemplary embodiments in accordance with the teachings of the present invention. Fig. 1a shows a withdrawal transaction in accordance with the teachings of the present invention. A user 11 is shown on the left interacting through data communication means with a bank party 12 on the right. A single transmission shift is shown because it is preferred for all the carry sub-protocols to be conducted in parallel, as would be appreciated by those of skill in the art. In general, however, whatever patterns of interaction between parties can be used.

Fig. 1b shows a payment interaction involving three parties, a user 11 making a payment to a payee 13 and additionally communicating with a bank 12. In one example transaction type, the payee 13 contacts the bank 12 after receiving information from the user 11, returns the result to the payer 13, and upon receiving a response from the user 11, is able to verify the payment. The user 11 has first supplied preferably all the possible borrow sub-protocol messages to the payee 13, who forwards these to the bank 12. Also forwarded can be the actual money numbers for the payment to the payee 13, but the authenticators are supplied by the user 11 only after receiving from the payee 13 the results of the payee's interaction with the bank 12. In a self-authenticating signature type of blinding, the payee name could be built into these money numbers in known ways so that the authenticators and a way to re-create the money numbers would be sufficiently convincing to the payee 13. For non-self-authenticating authenticators, the bank 12 might provide the payee 13 with a (possibly signed) image under a one-way function of the authenticator corresponding to a particular money number. This would then allow the payee 13 to become convinced upon receiving the authenticator from the user 11.

Turning now to Fig. 2, a detailed exemplary combination flow, functional, and protocol diagram of a maybemerge transaction is presented, in accordance with the teachings of the present invention. The arrow notation shown is well

known in the art and used in subsequent figures. The words "user" and "bank" serve to label the parties shown on their respective sides (although the reference numerals from Fig. 1 will not be cited for clarity). The upper, right-pointing arrow is labeled (as are all labels in this notation) with the essential message content communicated by the payment system user to the bank. The lower, left-pointing arrow shows messages returned in the opposite direction.

The upper arrow shows three components being sent. If the user does not wish to do the merge, then all three can be chosen by the user as random numbers—such as pseudorandom, physically random, or some combination. If the user does, however, wish to do the merge, then each of the three is preferably properly formed as follows: The first two are "money numbers," or unauthenticated identifiers of electronic coins, as are well known in the art. For instance, these could be the output of a one-way function applied to various values, numbers of a particular agreed and preferably standardized redundant format, or one of many other forms known in the signature and/or authenticator art, any identification of the coin being applicable. The first is denoted m_1 and the second m_2. The third and final value transferred is a blinded money number. It is shown as a blinding function "b" applied to a money number m_3, but any blinding scheme or functional equivalent could be used.

Before the bank returns the values of the second arrow, a check and preferably atomically combined database update is performed on the money number m_1 and m_2. The check is to ensure that the money number has not been previously spent; the update is to ensure that it cannot be spent later. These two operations are preferably performed as a single atomic action or in another way to provide that the number cannot be used between the time that it is checked and when it is blocked for further use. Such checks and atomic updates being well known in the art of electronic money as the process steps needed to ensure that coins cannot be spent more than once in an online transaction. If the check indicates that the number has been spent or the blocking does not succeed, then the bank will return an error, otherwise the bank will return the value shown on the arrow.

This single value shown returned by the second arrow is again for clarity in the example paradigm of the original blind signatures, but without limitation. It comprises three factors in a multiplicative group type of cryptosystem, as are well known in the art. The first and second factors are the images under two distinct one-way functions, f_1 and f_2, with their respective pre-images being the authenticator for m_1, shown as $a(m_1)$ and the authenticator for m_2, shown similarly. While these authenticator functions "a" are shown for clarity, any scheme for authentication or functionally equivalent construction could be used. The third factor is the authenticator function "s", in this case preferably having twice the value of a, applied to the blinded form of m_3, also as already described.

When the user obtains this number, it will be useless if the original input supplied by the user was random, as mentioned above. This is the case when no merge takes place. As will be appreciated, however, the bank does not know which case the user has chosen. Now when the user has formed the message properly, as described above, then the user will be able to recover the authenticator function applied to the result of the blinding function applied to m_3, or the functional equivalent in any blinding-like signature or authenticator scheme. For instance, in the scheme shown, the user knows the two authenticators, $a(m_1)$ and $a(m_2)$, as already mentioned, and so is able to apply the respective one-way functions to them. The multiplicative inverse of the resulting product can then by used to cancel these two factors from the message of the second arrow. The result is simply the desired signature $s(b(m_3))$, which is any data that effectively allows the user to develop an authenticator with twice the value of each of the authenticator types known for m_1 and m_2.

Referring now to Fig. 3, a detailed exemplary combination flow, functional, and protocol diagram of a maybesplit transaction is presented, in accordance with the teachings of the present invention. Much is the same as with Fig. 2, as

would be appreciated by those of skill in the art. One, instead of two, money numbers are provided along with two, instead of one, blinded money number. The result is two values, each containing a different one-way function of the authenticator for the first component as a factor with the desired authenticator for the blinded value.

More specifically, again the user forms the message, the bank checks and blocks the single money number m_1, and if no error computes the two different and preferably independent one-way functions f_1 and f_2 applied to the authenticator it calculates for m_1. When the bank returns the two authenticators that if forms for m_2 and m_3, each is multiplied by the respective one-way function image. Again, random input gives the payer nothing, although the bank won't know.

Referring now to Fig. 4, a detailed exemplary combination flow, functional, and protocol diagram of a general transformation transaction is presented, in accordance with the teachings of the present invention. As would be appreciated, this is a generalization of the schemes shown in Fig. 2 and 3. The two arrows are as in the previous figures, while the expression in brackets simply introduces notation. Instead of sending only one or two money number in raw form, the user sends some number k of them. Similarly, instead of sending one, or alternatively, two blinded money numbers, n such numbers are sent.

Various labels q are defined by the parenthetical expression. The first, shown explicitly, is q_j, which is a unique one-way function applied to a collection of authenticators and, in general, other labels q. Thus, the q's each represent a composition of one-way functions applied to various money numbers. The values sent back, in general, each are a product of a q and a signing function applied to a blinded money number. Thus, any combination of the input money numbers can be sufficient to yield each corresponding particular signature.

Turning now to Fig. 5, a detailed exemplary combination flow, functional, and protocol diagram of a preparatory transaction is presented, in accordance with the teachings of the present invention. The user is shown supplying a triple of blinded values, C, D and E. Each of these is subscripted by i to indicate that in general a number of such triples would be supplied, in whatever order. For instance, they might be supplied initially when an account is set up or to refill it periodically. For clarity in exposition, however, the lower-case variable names without subscript are also used here in describing particular instances of the transactions, without loss of generality.

What is shown being returned in the lower arrow is a pair of values, one for c and one for d. The first value, that for c, comprises the product of two values in some suitable structure, such as that substantially comprising a group in which the group operation and at least inverses are readily computed. The first value is the application of a suitable transformation, shown as one-way function f_1, to an x authenticator of the supplied blinded e. The other is the u authenticator of the supplied blinded c. In a similar way, the second part of the returned message is the product of two parts, one being f_2 applied to the x authentication of the blinded e and the other being the u authentication of the blinded d. This structure, as will be appreciated, is intended to provide that if the user obtains the x authenticator of e, then the user can obtain the u authenticator of c and d.

Turning now to Fig. 6, a detailed exemplary combination flow, functional, and protocol diagram of a maybesplit transaction using prepared coins is presented, in accordance with the teachings of the present invention. The first message shown is form the user to the bank, envisioned for instance to be through the payee during a payment transactions. In one case, as will be appreciated, it simply comprises random dummy values, except that e has the required redundancy or other property making it a potential coin apart from its authenticator. But in the case of an actual split, this first message comprises differently blinded forms of the two result coins c and d as well as the unblinded form of e. The blinding is

preferably substantially independent of that used in the corresponding preparatory instance of Fig. 5, so that the bank cannot readily link the two transactions.

The returned value shown in the second arrow, being from the bank to the user, comprises three components. All three components are formed including an encryption of the *w* authenticator of the *e*, each shown using a different version of *f*, as indicated by the subscripts 3, 4, and 5. The first component is the *x* authenticator of *e*, which allows the two components returned, as already described with reference to Fig. 5, to be opened. The second and third components allow the *v* authenticator of *d* and *c*, respectively, to be recovered. It is the combination of the *u* and *v* authenticators that are considered to be the proper authenticator for each of the split coin values. Preferably, the user can combine the two authenticators into one, such as by multiplying them in a discrete-log based system, yielding the sum of the exponents, and this sum is also the same authenticator used to issue coins of this denomination.

All manner of variations, equivalents, and adaptations can readily be conceived by those of skill in the art. Anticipated are all manner of re-arrangements and cryptographic variations, exploiting equivalent forms of information and cryptographic techniques. As one example, consider applying an invertible cryptographic operation to the authenticator protected before X-OR'ing in a plaintext version of the unlocking authenticator. As another example, various ways to condense the locking-factors and share variants of them across instances are possible, such as having the basic authenticator determine the seed of a sequence whose values are used as the locking parameters. Self-authenticating as well as merely authenticating techniques can be variously applied. Other basic approaches to preventing payee anonymity can be applied. As yet another illustrative example, some sort of tax could be assessed during at least some transformation transactions that applies only when the transaction is actually consumated.

While these descriptions of the present invention have been given as examples, it will be appreciated by those of ordinary skill in the art that various modifications, alternate configurations and equivalents may be employed without departing from the spirit and scope of the present invention.

* * * * *

What is claimed is:

1. A digital transaction system comprising:

at least one issuer of value;

at least one receiver of value;

at least two transacting parties issued value from said at least one issuer of value and providing at least parts of said value to said receiver parties; and

at least one transacting party combining, responsive to transacting with one of said issuer parties, items of value obtained from said issuer party, and supplying the item of combined value to a one of said receiver parties, while substantially hiding from the issuer party whether the combining has taken place.

2. A digital transaction system comprising:

at least one issuer of value;

at least one receiver of value;

at least two transacting parties issued value from said at least one issuer of value and providing at least parts of said value to at least said one receiver parties; and

at least one transacting party splitting, responsive to transacting with one of said receiver parties, items of value obtained from said issuer party, and supplying at least one of the resulting split items of value to the receiver party, while substantially hiding from the receiver party whether the splitting has taken place.

3. In the system of claim 2, the improvement comprising:

setup data shared between said issuer of value and said transacting party;

said transferring value by at least one of said transacting parties from said issuer party to at least one said receiver party, including said transacting party changing denominations of value in such a way that the transacting party is substantially constrained to provide value in a form that is determined by said setup data.

4. A digital system for exchanging value comprising:

at least one issuer of value;

at least one receiver of value;

at least two transacting parties;

at least one transacting party accomplishing transactions of value between at least one issuer and at least one receiver of value while changing the denominations of coins issued and preserving the aggregate value, such that the transacting party can substantially keep the other parties to the transaction from learning what denominations were changed.

5. In the exchange of value of claim 4, the improvement comprising: a merge transaction in which the transacting party hides which of two cases pertains: the merge between two coins involves bogus coins or the merge involves genuine coins.

6. In the exchange of value of claim 4, the improvement comprising: a split transaction in which the transacting party hides which of two cases pertains: the split of a coin into two involves bogus coins or the split involves genuine coins.

7. In the exchange of value of claim 4, the improvement comprising: said transacting party being constrained to introduce new coins only from a pre-arranged batch of coins from which the original coins were obtained.

8. In the exchange of value of claim 4, the improvement comprising: said transacting party being able to spend the full amount of value held.

9. In the exchange of value of claim 4, the improvement comprising: said transacting party being able to maintain between transactions value in coin denominations of a canonical form.

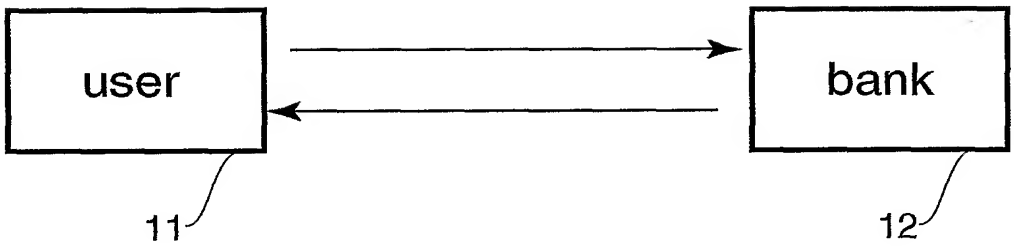


Fig. 1a

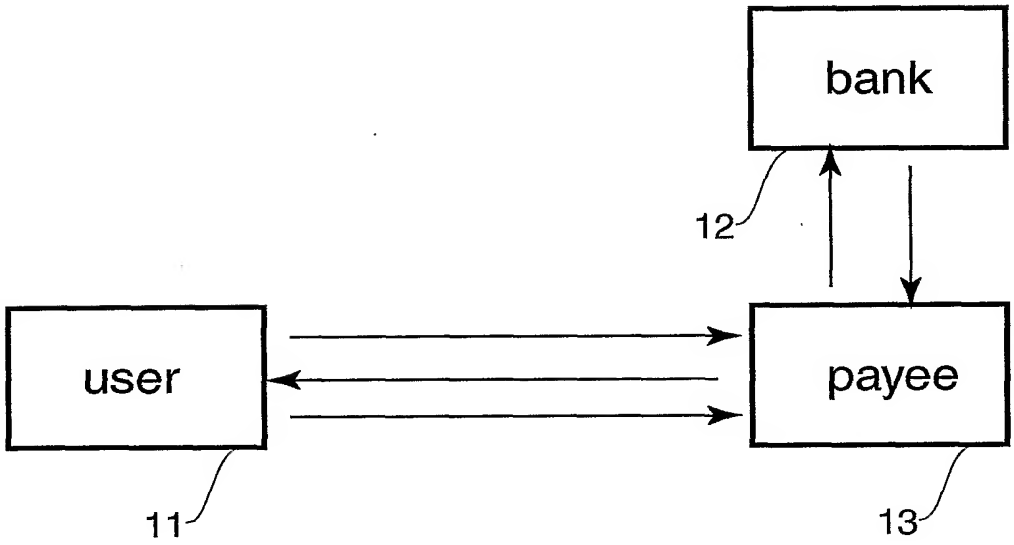


Fig. 1b

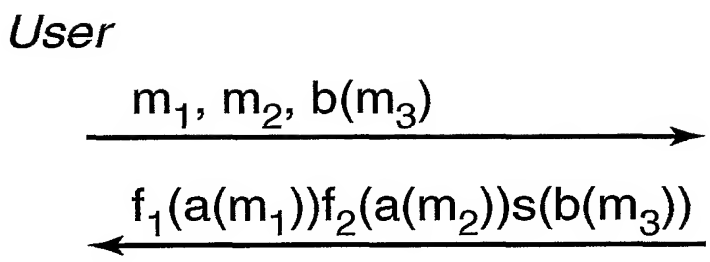


Fig. 2

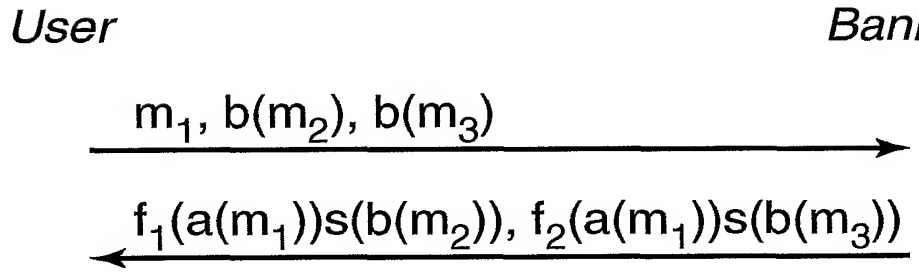


Fig. 3

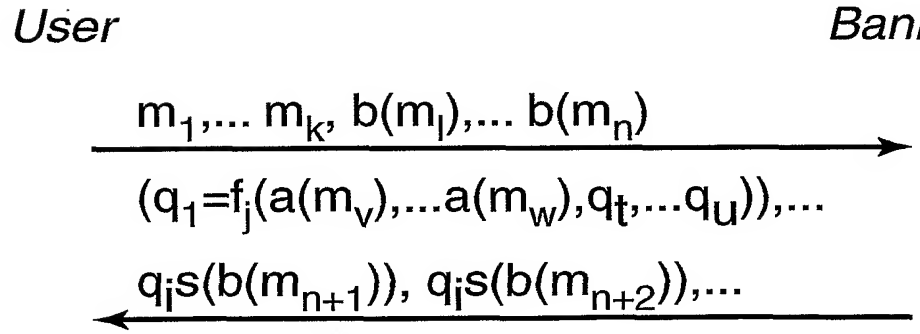


Fig. 4

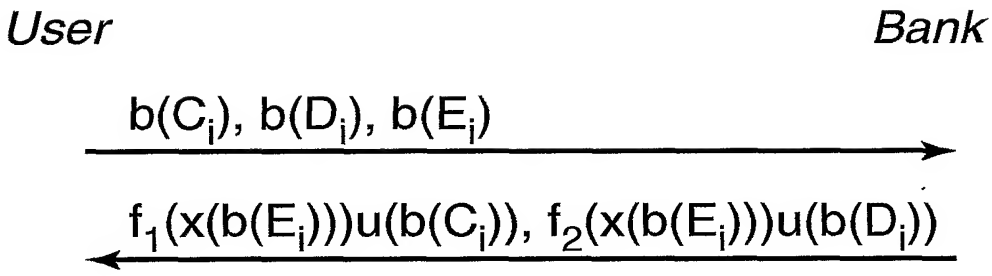

User
Bank
b(C_i), b(D_i), b(E_i)
f_1(x(b(E_i)))u(b(C_i)), f_2(x(b(E_i)))u(b(D_i))

Fig. 5

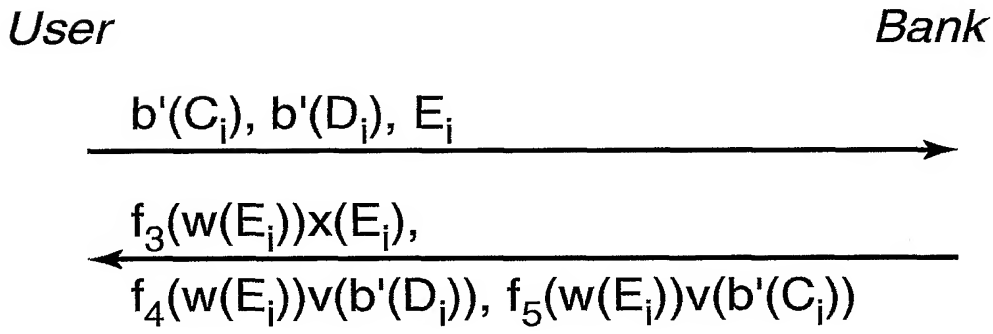

User
Bank
b'(C_i), b'(D_i), E_i
f_3(w(E_i))x(E_i),
f_4(w(E_i))v(b'(D_i)), f_5(w(E_i))v(b'(C_i))

Fig. 6